AMENDMENTS TO THE SPECIFICATION

1. Please replace paragraph **[0034]** with the following amended paragraph **[0034]**:

[0034] As illustrated, Security processor (CPU) 114 is connected between ISO processor (CPU) 112 and sensor 110 for providing secure processing and storage of the captured data, as well as a secure "firewall" to protect the data and programs stored in its dedicated memory from any improper access attempt via the ISO processor 112, as will be described hereinafter. Such a firewall may be designed to pass only encrypted data using an encryption key which is based on a uniquely assigned network address or that otherwise is unique to the particular card, such as data extracted from a previously stored fingerprint pattern or a uniquely assigned device number such as CPU number or a fingerprint sensor number. In another embodiment, the Firewall only passes data which contains unique identifying data from a previous transmission, or data. In yet other embodiments, the Firewall maintains different keys for different applications, and uses those keys to route the data to a respective different processor or memory partition.

2. Please replace paragraph **[0043]** with the following amended paragraph **[0043]**:

[0043] The application server 202 includes functionality for conducting a transaction or otherwise responding to instructions from the remote user at client terminal 200 after the user's identity has been verified by authentication server 204. The authentication server 204 includes functionality for secure communication with both client terminal 200 and application server 202, for storing authentic fingerprint data and other information concerning previously registered users, for comparing the stored data with the encrypted live data received from the client terminal 200, and for advising the application server 202 whether ~~202whether~~ or not specified live fingerprint data matches specified stored fingerprint data.

3. Please replace paragraph **[0045]** with the following amended paragraph **[0045]**:

[0045] Application Server 202 further comprises an internet server interface including the firewall 206 and internet browser 214, as well as a transactional application module 216 and a validation module 218. In the event the application server and application module 216 are legacy devices that were not designed to communicate externally by means of the IP/TCP protocol, the firewall 206 can be replaced with an appropriate protocol converter which incorporates the validation module 218 and which has a fixed IP address. Application ~~Service~~ Server may for example be operated by a third party who is willing to provide service through Internet to an authorized User.

4. Please replace paragraph **[0060]** with the following amended paragraph **[0060]**:

[0060] An exemplary preferred embodiment utilizing a Three Way Authentication Protocol and a Onetime Password as a Hash Character Encoding Sequence will now be described with reference to FIG. 3:

- Web Browser 210 of Client Terminal 200 accesses the corresponding Web Interface 214 of Application Server 202 with a request to access Application Process (module) 216.
- Web Interface 214 of Application Server 202 responds with LOG-IN screen information and related instructions for accessing Application Process 216.
- Client Terminal 200 instructs ISO Processor 112 to activate Security Processor 114.
- ISO Processor 112 triggers Security Processor 114.
- Security Processor 114 awaits Fingerprint Data from Fingerprint Sensor 110 and when valid data is received, extracts a digital Fingerprint Pattern which is forwarded to Web Browser 210 via ISO Processor 112.
- Web Browser 210 sends an encrypted version of the extracted Fingerprint Pattern to Authentication Server 204 accompanied by (or encrypted with) Related Information about the involved Card 100' and Card Reader 208, such as User ID, IP address of Client Terminal 200, and/or hardwired ID code (MAC address) of Sensor 110.

• Web Interface 220 of Authentication Server 204, upon receiving the extracted Fingerprint Pattern along with the other information from Client Terminal 200, forwards that information to the Fingerprint Matching Processor 222.

• Under the control of Matching Software 224, Fingerprint Matching Processor 222 uses the received User ID or other User specific Related Information to retrieve a corresponding reference Fingerprint Pattern from Database 226 and compares the captured Fingerprint Pattern to the reference Fingerprint Pattern.

• The result (Matched or Unmatched) is stored in an Access History log together with the Related Information identifying the Terminal 200, User ID Card 100' and requesting Application Process 216, and control is returned to Authentication Server Web Interface 220.

• If the result is Matched, Authentication Server Web Interface 220 then generates a One Time Password in the form of a Challenge Character Sequence which is transmitted to Client Terminal 200, and uses that Challenge Character Sequence as a Hash code to encrypt the Related Information which it saves as the corresponding Challenge Response for possible future reference.

• Client Terminal 200 uses the received Challenge Character Sequence as a Hash code to encrypt a previously stored unencrypted copy of the submitted Related Information, which it then forwards to the Web Interface 214 of Application Server 202 as part of its response to the Application Log-In Process.

• Web Interface 214 of Application Server 202 upon receiving Hash converted Related Information, forwards it to the Application ~~Service~~ Process 216 which associates it with an on going Log-On attempt from that Client Server, and, for the purpose of confirming the Matched result, forwards the received Related Information which was Hashed by the Client Terminal using the Challenge Sequence provided by the Authentication Server as Challenge Response.

• The Web Interface 220 of Authentication Server 204, upon receiving the Challenge Response from the Application Server, forwards that Response to the Authentication Process 222 which compares it with its previously saved reference copy of the expected Challenge Response to determine whether the User's Identity has in fact been authenticated.

• Any authenticated User Identity information resulting from that comparison is then returned to the Application Process 216 via the Authentication Server Web Interface 220 and the Validation Interface 218 of Application Server 202.

• Validation Interface 218 uses the Authentication to confirm the User's Identity as established in the original Log-On attempt has been validated.

• Once the User's Identity has been confirmed, Application ~~Authentication~~ Process 216 then proceeds to communicate directly with Web browser 210 of Client Terminal 200 via Web Interface 214 of Application Server 202.

5. Please replace paragraphs **[0062] -[0063]** with the following amended paragraph **[0062] - [0063]**

[0062] When a SmartCard 100 is inserted in Card Reader 208, a reset signal RST is sent from the card reader to both ISO CPU (START block 502) and Security ~~Fingerprint~~ CPU 114 (Fingerprint Verification block 504) and both receive power VCC from the Card Reader 208. ISO CPU then responds with ATR (Answer-to-Reset) message and communicates PPS (Protocol and Parameters Selection) as needed (block 506). At the same time, Security ~~Fingerprint~~ CPU goes into waiting state for receiving Fingerprint data and when data is received from sensor 110, performs the authentication process (block 504).

[0063] When an initial request command is sent by the Application Process 216 to ISO CPU 112 (block 508) the ISO CPU queries (block 510) Security CPU about the authentication status. If the response is positive, ISO CPU responds to the application by executing the requested command (block 512). Otherwise (either an error message or no response from Security CPU 114) it does not make any response to the requested command but rather waits for a new first request (block 508b).

6. Please replace paragraph **[0065]** with the following amended paragraph **[0065]**:

[0065] FIG. 7 is similar to the flowchart of FIG. 6, but modified for use with the exemplary biometric verification card of FIG. 5. The far left hand side of FIG. 7 shows

the functions performed by Application Server 202, the next column corresponds to Reader 208, the next column depicts ISO contacts 108, the next column shows functions performed by Security CPU 114, while the far right hand side shows the functions performed by an unmodified ISO SmartCard CPU 112.

- When either a SmartCard is inserted in a card reader or the application software starts operation of card reader device, a Reset Signal 550 is sent from Card Reader 208 to Security CPU 114.
- Soon after Security CPU receives Reset Signal 550, it sends a corresponding Reset Signal 552 to ISO CPU 112. Concurrently Security CPU awaits Fingerprint data from Fingerprint Sensor.
- Upon receipt of Reset Signal 552, ISO CPU makes an ATR (Answer-to-Reset) response 554 and thereafter communicates PPS (Protocol and Parameters Selection) as needed.
- As soon as Security CPU 114 ~~CPU r114~~ receives ATR (Answer-to-Reset) from ISO CPU, it transfers it to Card Reader (block 556), including any associated PPS commands.
- In the meantime, if Security CPU receives fingerprint data, it executes the previously described authentication process. In the event the authentication test results in a PASS, the pass status is maintained for specific time period. If the result is FAIL, Security CPU 114 awaits new fingerprint data.
- Upon the application execution, a command request 558 is sent to Security CPU, which transfers a command request 560 to ISO CPU and also transfers its correct response 562 to Card Reader only if the Security CPU is still in the previously mentioned PASS state or if the last correct response had More-data bit set (test block 564).
- Otherwise (No branch 566) Security ~~Fingerprint~~ CPU generates a dummy request 568 and transfers it to ISO CPU and also transfers the resultant ERR response 570 to the Application Process 216 via Card Reader 208 ~~216~~, thereby maintaining proper synchronization between the sequence numbers in the requests and responses.

7. Please replace paragraph **[0072]** with the following amended paragraph **[0072]**:

[0072] ISO antenna 132 comprises two loops generally located about the periphery of card 100 and provides an ISO-compatible wireless interface to ISO CPU 112 for both data and power similar to that afforded by the wired electrical interface 108. In addition, a Security antenna 130 ~~134~~ (in the depicted example, inside antenna 132 and consisting of only one loop) provides a separate source of power to Security CPU 114 via a DC-DC power regulator 120. Because the there is no direct connection for wireless data except through ISO CPU 112, the sensitive data stored within Security CPU 114 is not compromised by such a wireless interface. Alternatively, as mentioned previously with respect to the embodiments having only wired connections to the external reader and external network, the functionality of the two processors could be combined, or the external interface could be through the Security CPU 114 rather than the ISO CPU 112, in which appropriate wireless security measures would have to be incorporated into the thus-modified architecture.